COMMONWEALTH
OFFICE OF
TECHNOLOGY

COT Security Alert – Microsoft Vulnerability Related to Duqu Malware

A malware known as Duqu has been in the news recently being touted as the next Stuxnet due to each containing similar source code. Recent information says that several organizations in Europe and the Middle East have possibly been infected with Duqu.

Microsoft is investigating a Win32k TrueType font parsing engine component vulnerability that is related to this malware. The vulnerability would allow a successful attacker to run arbitrary code in kernel mode potentially allowing them to install programs, access and change or delete data or create user accounts with full user rights. Until a patch is released by Microsoft to address this vulnerability users are advised to remember **never to open attachments from unknown senders and to verify unexpected attachments from known senders before opening**. The vulnerability cannot be exploited automatically via email unless the user opens an infected attachment sent in an email message.

More information on the Microsoft vulnerability may be found at technet.microsoft.com/en-us/security/advisory/2639658.

More information on W23.Duqu may be found on a Symantec report found at www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf.

Forwarding this email to users will result in an increase of awareness.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Security Administration Branch
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServicesISS@ky.gov
http://technology.ky.gov/ciso/